Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application. Applicants have submitted a new complete claim set showing any marked up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing.

Listing of Claims:

1. (Currently Amended) A hardware-implemented computer system for processing e-mail comprising:

a plurality of servers that receive e-mail messages from a plurality of remotely located clients, the plurality of servers being part of a distributed network;

a plurality of packet sniffers, wherein each of the packet sniffers in the plurality of packet sniffers corresponds to and resides in a different server in the plurality of servers, wherein each packet sniffer in the plurality of packet sniffers is configured to; a) check a fragment offset field of an IP header to ensure the IP header is the first fragment of a packet, b) determine the value of a SYN bit in a TCP header, c) disregarding the packet if the SYN bit has not been set, and if the frame does not include an IP address, and if the IP address does not correspond to the server on which the packet sniffer is running, and if the IP address does not correspond to the configured port number and d) extract from the received packet originating IP addresses associated with e-mail messages that are communicated to the clients over the distributed network;

a central monitor that communicates over the distributed network with the plurality of packet sniffers and that monitors data regarding the originating IP addresses, wherein the central monitor is configured to determine whether traffic from an originating IP address has exceeded a

threshold value, the central monitor being further configured to generate a response to detect spam e-mail messages if the threshold value has been exceeded; and

a server in which the central monitor resides, wherein the server is distinct from each of the plurality of servers containing the plurality of packet sniffers in the plurality of packet sniffers in the distributed network.

2. (Currently Amended) The hardware-implemented system of claim 1 wherein each of the servers further includes a blacklist containing IP addresses that have been determined to be generating spam e-mail messages; and

wherein each server checks the originating IP addresses of incoming connections to the addresses contained in the blacklist, and rejects any connection originating from an address on the blacklist.

3. (Currently Amended) The hardware-implemented system of claim 1 wherein each of the servers further includes a message switch that determines whether e-mail messages are spam, and communicates e-mail messages to clients.

4. (Canceled)

5. (Currently Amended) The hardware-implemented system of claim 3 further comprising:

a spam database for storing rules for determining whether e-mail messages are spam;

wherein the message switch determines whether e-mail messages ~~are~~ are spam based on the rules within the spam database.

6. (Currently Amended) The hardware-implemented system of claim 5 wherein each rule in the database is assigned a score that is used to determine whether an e-mail message is spam.

7. (Currently Amended) The hardware-implemented system of claim 6 wherein the response generated by the central monitor comprises raising the score of a rule corresponding to the originating IP address.

8. (Currently Amended) The hardware-implemented system of claim 1 wherein the response generated by the central monitor comprises an alert that is communicated to a spam analyst.

9. (Currently Amended) The hardware-implemented system of claim 2 wherein the response generated by the central monitor comprises a command to add the originating IP address to the blacklist.

10. (Currently Amended) The hardware-implemented system of claim 1 wherein the threshold value comprises a rate parameter.

11. (Currently Amended) The hardware-implemented system of claim 1 wherein the threshold value comprises a maximum total connections parameter.

12. (Currently Amended) The hardware-implemented system of claim 1 wherein the central monitor determines whether an originating IP address has exceeded a threshold value by use of a token bucket algorithm including a rate parameter and a maximum connections allowed parameter.

13. (Currently Amended) A hardware-implemented system for detecting spam e-mail messages in a distributed network including a plurality of servers that receive and process e-mail messages for a plurality of different remotely located clients, the system comprising:

a plurality of packet sniffers, each of which is located on a unique one of the plurality of servers, such that each of a plurality of packet sniffers are configured to; a) check a fragment offset field of an IP header to ensure the IP header is the first fragment of a packet, b) determine the value of a SYN bit in a TCP header, c) disregarding the packet if the SYN bit has not been set, and if the frame does not include an IP address, and if the IP address does not correspond to the server on which the packet sniffer is running, and if the IP address does not correspond to the

configured port number and d) extract originating IP addresses associated with e-mail messages that are communicated to clients by the server;

a central monitor that communicates with the plurality of packet sniffers and that monitors data regarding the originating IP addresses, wherein the central monitor is configured to determine whether traffic from an originating IP address has exceeded a threshold value, the central monitor being further configured to generate a response to detect spam e-mail messages if the threshold value has been exceeded; and

a server in which the central monitor resides, wherein the server is distinct from each of the packet sniffers in the plurality of packet sniffers in the distributed network.

14. (Currently Amended) The hardware-implemented system of claim 13 wherein the central monitor resides on a server separate from the packet sniffers.

15. (Currently Amended) The hardware-implemented system of claim 13 further comprising:

a blacklist stored on each of the servers, the blacklist including IP addresses that have been determined to be generating spam.

16. (Currently Amended) The hardware-implemented system of claim 13 further comprising:

a spam database that stores rules for determining whether e-mail messages are spam; and

a message switch that determines whether e-mail messages are spam based on the rules within the spam database.

17. (Currently Amended) The hardware-implemented system of claim 16 wherein each rule in the database is assigned a score that is used to determine whether an e-mail message is spam.

18. (Currently Amended) The hardware-implemented system of claim 17 wherein the response generated by the central monitor comprises raising the score of a rule corresponding to the originating IP address.

19. (Currently Amended) The hardware-implemented system of claim 13 wherein the response generated by the central monitor comprises an alert that is communicated to a spam analyst.

20. (Currently Amended) The hardware-implemented system of claim 13 wherein the response generated by the central monitor comprises a command to the system to block future e-mail messages from the originating IP address.

21. (Currently Amended) The hardware-implemented system of claim 13 wherein the threshold value comprises a rate parameter.

22. (Currently Amended) The hardware-implemented system of claim 13 wherein the threshold value comprises a maximum total connections parameter.

23. (Currently Amended) The hardware-implemented system of claim 13 wherein the central monitor determines whether traffic from an originating IP address has exceeded a threshold value by use of a token bucket algorithm including a rate parameter and a maximum connections allowed parameter.

24. (Currently Amended) A method for processing e-mail and detecting spam e-mail messages, comprising:

routing the e-mail messages through a distributed network including a plurality of servers that receive and process e-mail messages for a plurality of different remotely located clients;

communicating the processed messages to the plurality of remotely located clients by use of the plurality of servers;

a) checking a fragment offset field of an IP header to ensure the IP header is the first fragment of a packet, b) determining the value of a SYN bit in a TCP header, c) disregarding the

packet if the SYN bit has not been set, and if the frame does not include an IP address, and if the IP address does not correspond to the server on which the packet sniffer is running, and if the IP address does not correspond to the configured port number and d) extracting, at the plurality of servers, originating IP addresses associated with e-mail messages that are communicated to the plurality of remotely located clients;

monitoring data regarding originating IP addresses;

determining whether traffic from an originating IP address has exceeded a threshold value; and

generating, at a central monitor, a response for use in detecting spam e-mail messages if the threshold value has been exceeded.

25. (Original) The method of claim 24 further comprising:

storing data regarding the originating IP addresses in a database.

26. (Original) The method of claim 24 further comprising:

maintaining a list of acceptable IP addresses;

checking originating IP addresses against the list; and

determining whether traffic from an originating IP address has exceeded a threshold value only if the originating IP address is not in the list.

27. (Original) The method of claim 24 wherein the threshold value comprises a rate parameter.

28. (Original) The method of claim 24 wherein the threshold value comprises a maximum total connections parameter.

29. (Original) The method of claim 24 wherein determining whether traffic from an originating IP address has exceeded a threshold value is performed by use of a token bucket algorithm including a rate parameter and a maximum connections allowed parameter.

30. (Original) The method of claim 24 further comprising:

storing IP addresses that have been determined to be generating spam in a blacklist;

checking originating IP addresses of incoming connections to the servers against the IP addresses contained in the blacklist; and

rejecting any connection originating from an IP address in the blacklist.

31. (Previously Amended) The system of claim 30 wherein the response generated by the central monitor comprises a command to add the originating IP address to the blacklist.

32. (Original) The method' of claim 24 further comprising:

storing rules for determining whether e-mail messages are spam in a spam database; and

determining whether e-mail messages are spam based on the rules within the spam database.

33. (Original) The method of claim 32 wherein each rule in the database is assigned a score that is used to determine whether an e-mail message is spam.

34. (Original) The method of claim 33 wherein generating a response comprises raising the score of a rule corresponding to the originating IP address.

35. (Original) The method of claim 24 wherein generating a response comprises communicating an alert to a spam analyst.

36. (Previously Amended) The system of claim 24 wherein the response generated by the central monitor comprises a command to the system to block future e-mail messages from the originating IP address.